Datentresor gegen Ransomware-Erpresser

Ransomware-Attacken verursachen weltweit jedes Jahr Schäden in Milliardenhöhe. Dell EMC hat seine Data-Domain-Serie daher um einen speziellen Schutz erweitert.

Ransomware ist in den vergangenen Jahren zur größten Malware-Bedrohung für Unternehmen geworden. Die Software verschlüsselt die internen Daten einer Organisation oder verwehrt den Usern den Zugriff darauf. Erst nach Zahlung der geforderten Summe geben die Erpresser die Daten wieder frei. Oder auch nicht: Oft kommt es vor, dass die Täter mit dem Geld untertauchen, ohne sich noch einmal zu melden. Doch egal, ob ein Unternehmen der Forderung nachkommt oder nicht: Der Schaden ist auf jeden Fall immens und erreicht teilweise dreistellige Millionenbeträge.

Die Methoden der Ransomware-Programmierer sind in den letzten Jahren immer raffinierter geworden und damit auch immer schwerer abzuwehren. Da Backups einen gewissen Schutz versprechen, greift die Schadsoftware mittlerweile oftmals gezielt die Sicherungssysteme des Unternehmens an, löscht sämtliche vorhandenen Daten und führt eine Neuinitialisierung der Systeme durch. Es sind daher neue Konzepte für den Schutz der Daten erforderlich.

Wie sich Unternehmen schützen können

Das amerikanische National Institute of Standards and Technology (NIST) empfiehlt Unternehmen einen mehrstufigen Schutz ihrer Daten. Er umfasst zum einen die klassischen Daten-Backups, wie sie heute glücklicherweise von praktisch allen Firmen vorgenommen werden. Hinzu kommen unter anderem regelmäßige Sicherungen der Daten auf einem speziell dafür ausgelegten Backup-Server, Berechtigungen für den Zugriff auf die Backups und die Definition dedizierter Backup-User sowie in der Praxis bewährte Konzepte wie die 3-2-1-Regel: Drei Kopien der Daten liegen auf zwei Medien, von denen eines extern gelagert wird.

Für Backups, die höchsten Ansprüchen an Sicherheit genügen, bietet Dell EMC die Modelle der Data-Domain-Reihe an. Die Maschinen speichern die Unternehmensdaten auf Disk, wobei es sich in erster Linie um Festplatten handelt, einige Modelle verfügen auch über SSDs. Um den vorhandenen Platz bestmöglich zu nutzen, werden die Daten von der Data Domain per Hardware dedupliziert. Die Maschinen eignen sich daher sowohl für die Aufnahme regelmäßiger Backups wie auch für die längerfristige Archivierung. Sie wurden zudem von vornherein auf höchste Sicherheit getrimmt und bieten dazu beispielsweise einen Retention Lock: Die Funktion sorgt dafür, dass die gesicherten Daten für einen einstellbaren Zeitraum weder verändert noch gelöscht werden können. Dabei unterstützt die Data Domain zwei unterschiedlich strenge Level: In der Variante Governance lässt sich der Retention Lock bei Bedarf aufheben. Ist jedoch die Variante Compliance eingestellt, funktioniert das nicht mehr, die Sperre ist dann bis zum Ende des eingestellten Zeitraums fest. Wählt der Anwender diese Option, erfüllt die Data Domain die Vorgaben der staatlichen Behörden für die sichere Aufbewahrung von Daten. Der Retention Lock der Data Domain wird unterstützt von den Backup-Anwendungen Dell EMC PowerProtect Data Manager und NetWorker sowie einigen Produkten anderer Hersteller.

Ein zusätzliches Sicherheits-Feature der Data Domain nennt sich DDBoost. Dabei handelt es sich um ein von Dell EMC entwickeltes Protokoll, das es ermöglicht, die Maschinen direkt in Backup-Anwendungen zu integrieren. In diesem Fall lässt sich die Deduplikation der Daten bereits auf dem Backup-Server beziehungsweise dem -Client durchführen. Dadurch reduziert sich die benötigte Netzwerkbandbreite und die Zeit für die Datenübertragung sinkt.

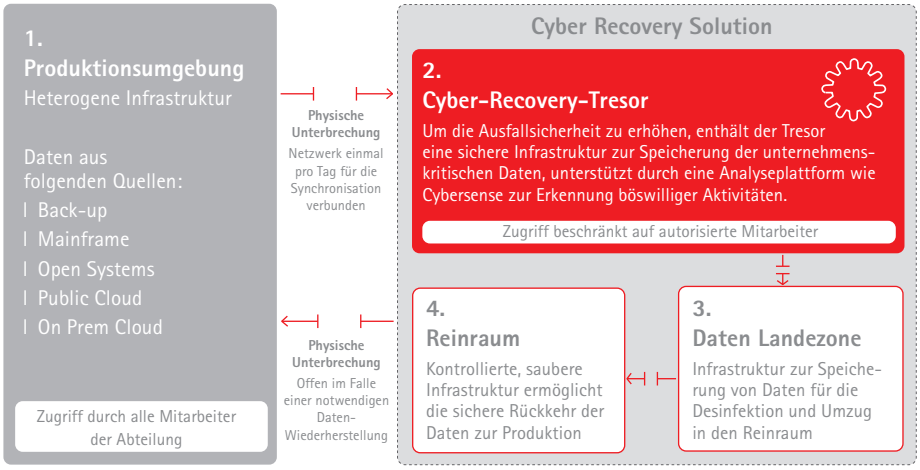
Erweiterter Schutz gegen Ransomware-Attacken

Aufgrund der steigenden Bedrohung durch Ransomware-Angriffe hat Dell EMC eine Schutz-Software entwickelt, die in ihrem Konzept und den Möglichkeiten derzeit einmalig ist. Cyber Recovery gehört zum Lieferumfang der neueren Data-Domain-Systeme und bildet eine Art letzter Verteidigungslinie gegen Malware-Angriffe aller Art. Denn auch eine Funktion wie der Retention Lock der Data Domain hat eine Schwachstelle: Sobald es einem Angreifer gelingt, das Backup-System selbst unter seine Kontrolle zu bekommen, ist er auch in der Lage, alle anderen User auszusperren. Dann ist es einem Unternehmen nicht mehr möglich, auf die Daten zuzugreifen.

Ausgehend von der Beobachtung, dass moderne Ransomware zunehmend auf die Backup-Systeme in den Unternehmen abzielt und danach trachtet, sie zu deaktivieren oder zu kontrollieren, entstand bei Dell EMC das Konzept für einen Vault, also einen Tresor, der für Angreifer absolut unzugänglich ist. Dieser Cyber Recovery Vault (CR Vault) speichert eine Art Goldkopie der Unternehmensdaten,

Wichtige strategische Überlegungen im Vorfeld eines Cyber-Recovery-Projektes.

sodass sich der vorherige Datenstand jederzeit wiederherstellen lässt. Mehr noch: Der Cyber Recovery Vault kann auch den Backup-Server selbst aufnehmen und auf diese Weise die Funktionsfähigkeit der Wiederherstellungsroutinen sicherstellen. Bei den Backup-Lösungen Dell EMC Networker und Data Manager lässt sich dieser Vorgang sogar automatisieren, bei anderen Sicherungsprodukten muss der Administrator den Server manuell aufsetzen. Dann ist es möglich, nicht nur die von der Malware blockierten Datensätze, sondern auch den fertig konfigurierten Server zurückzuspielen und



Schematische Darstellung der zentralen Elemente einer Cyber-Recovery-Umgebung.

auf diese Weise innerhalb kürzester Zeit wieder eine saubere und funktionierende Produktionsumgebung herzustellen.

Die Basis für Dell EMC Cyber Recovery bilden zwei Data-Domain-Systeme. Die eine Maschine ist in die Produktiv-Umgebung eingebunden, üblicherweise als Backup-Target. Sie repliziert ihre Daten auf die zweite Data Domain, den Cyber Recovery Vault. Dieser Vault steht in einem eigenen, abgeschlossenen Raum, zu dem nur ein ausgesuchter Personenkreis Zutritt hat – laut Statistik erfolgen die meisten Datendiebstähle in den Unternehmen durch interne Mitarbeiter. Er ist nicht an ein Netzwerk angeschlossen, sondern durch ein virtuelles Air Gap von allen anderen Systemen separiert. Damit im Rahmen der Replikation überhaupt eine Datenübertragung erfolgen kann, öffnet die Cyber-Recovery-Software auf der Data-Domain-Maschine im Vault über eine Policy den physischen Replikations-Port und überträgt die Daten vom Backup-Server zum Vault. Sobald sämtliche Daten ihr Ziel erreicht haben, wird die Verbindung von der Software wieder geschlossen.

Als zusätzliche Schutzfunktion ist im Cyber Recovery Vault ein Dateisystem eingerichtet, das jegliche Veränderung der Daten ausschließt (Write Once Read Many – WORM). So sind sie nicht nur vor Bearbeitungen geschützt, sondern gleichzeitig auch vor böswilligen Crypto-Verschlüsselungen, wie sie oft bei Ransomware-Angriffen eingesetzt werden.

Zusätzliche Analyse auf Malware-Befall

Ein großes Problem bei herkömmlichen Backup-Systemen ist, dass die Daten, die im Rahmen eines Recovery zurückgespielt werden sollen, ebenfalls bereits von einer Malware befallen sind. Antiviren-Software kann diese Gefahr minimieren, gänzlich ausschließen lässt sie sich jedoch nicht. Bei der Goldkopie der Daten eines Unternehmens wäre es besonders fatal, wenn sie aufgrund der Aktivitäten einer Malware unvollständig oder manipuliert oder sogar selbst befallen wäre. Da der Cyber Recovery Vault jedoch die meiste Zeit keine Verbindung mit der Außenwelt hat, ist es nicht möglich, dort eine Antiviren-Lösung zu einzurichten, die ständig aktuell mit Malware-Definitionen versorgt wird.

Um eine Veränderung oder Verunreinigung der Goldkopie so weit wie möglich auszuschließen, ist Dell EMC eine Partnerschaft mit dem US-Unternehmen Index Engines eingegangen, Hersteller der Security-Software CyberSense. Diese optional lizenzierbare Anwendung analysiert unstrukturierte Daten auf Merkmale und Veränderungen, die auf eine Malware-Infektion hinweisen. Dabei wendet sie sowohl heuristische Methoden wie auch Methoden des Machine Learning an und vergleicht zudem die auf dem Vault eingehenden Backup-Daten mit bereits bestehenden, älteren Datenbeständen. Die Software überwacht kontinuierlich die ankommenden Daten und sucht beispielsweise nach Auffälligkeiten in der Bit-Struktur und Hinweisen auf Verschlüsselungen. Außerdem achtet sie auf den Anteil von veränderten Daten in den eingehenden Backup-Sätzen – wenn sich dieser Prozentsatz plötzlich deutlich verändert, schlägt sie sofort Alarm. Die Benachrichtigung des zuständigen Administrators erfolgt dann per SMTP, also per E-Mail. Auf diese Weise lassen sich Verunreinigungen der Goldkopie oftmals noch verhindern. Sollten dennoch veränderte oder verschlüsselte Daten in den Cyber Recovery Vault gelangt sein, lassen sie sich mit CyberSense durch ältere Kopien ersetzen.

Individuell anpassbar

Die Kombination aus Data-Domain-Maschinen, Backup-Software, Dell EMC Cyber Recovery und Cyber Sense ist nicht fest, sondern lässt sich flexibel an das Budget und die Anforderungen des jeweiligen Unternehmens anpassen. Management und IT-Abteilung haben mehrere Optionen, beispielsweise ob die komplette Produktionsumgebung in der Vault gesichert werden soll oder ob es genügt, die wichtigsten Unternehmensdaten vor dem Zugriff von Kriminellen zu schützen. Das ist nicht nur eine Kostenfrage, sondern auch eine Frage der Recovery-Geschwindigkeit: Das zusätzliche Backup der Produktionsumgebung erfordert zwar ein größeres Speichervolumen, erspart jedoch ein Neuaufsetzen des gesamten Systems und verkürzt damit die Zeit, bis die IT wieder zur Verfügung steht.

Dell EMC Cyber Recovery stellt derzeit den wohl wirksamsten Schutz gegen den Versuch der Erpressung durch das Einschleusen von Ransomware dar. Die Software erfordert jedoch eine gründliche Analyse der Situation beim Kunden und eine eingehende Beratung. Die GID GmbH bietet daher entsprechende Consulting Services an. Sie umfassen unter anderem Workshops vor Ort beim Kunden, Analysen des derzeitigen und des gewünschten, zukünftigen Status, die Entwicklung einer Strategie zusammen mit dem Kunden sowie die Integration der angepassten Lösung in die Data-Protection-Umgebung des jeweiligen Unternehmens. Unternehmen bekommen auf diesem Weg genau die Cyber-Recovery-Lösung, nach der sie verlangen und die sie benötigen.

Kontakt

GID GmbH
Brügelmannstr. 5, 50679 Köln
Tel. +49 221 83 79 02-0, info@gid-it.de
www.gid-it.de